



UNITED STATES MARINE CORPS

3D MARINE DIVISION (-) (REIN)

UNIT 35801

FPO AP 96602-5801

In reply refer to
DivO 5271.3

G-6

26 JAN 2000

DIVISION ORDER 5271.3

From: Commanding General
To: Distribution List

Subj: TERMINAL AREA SECURITY OFFICER (TASO)

Ref: (a) IRM-5239-06 Data Access Security
(b) Computer Fraud and Abuse Act 1986
(c) IRM-5234-04 Naming Conventions
(d) IRM-5239-08 Computer Security Procedures
(e) DivO 5271.1A

Encl: (1) Computer Security Organizational Elements
(2) Sample Terminal Area Security Officer Appointment Letter
(3) Computer Fraud and Abuse Act of 1986

1. Purpose. To establish policy, provide guidance, and prescribe specific responsibilities of Terminal Area Security Officers in accordance with references (a) through (d). Enclosure (1) depicts the organizational elements primarily tasked with computer security as defined in paragraph 4.

2. Background. During the past five years, computer use has increased exponentially. Technology has continued to evolve providing more users the opportunity to access computers and data files. As a result, the threat to unit security and sensitive data has also increased. Recent media coverage of computer crime, espionage, and youthful "hackers", coupled with Public Law 100-235, "Computer Security Act of 1986" and the establishment of the National Computer Security Center (NCSC), has raised the level of computer security awareness in government, DoD, industry, and the general population.

3. Policy. The safeguarding of sensitive information against unauthorized access, modification, destruction, or denial of use is a computer security issue that requires the greatest degree of coordination and cooperation at all levels of command. In that regard, all commanders and principle staff officers will ensure that the contents of this order are implemented and complied with.

4. Definitions

a. Computer Systems Security Officer (CSSO). The MCB Regional Automated Support Center (RASC) is required to appoint a CSSO who is responsible for the effective implementation of computer security procedures for all the Major Subordinate Commands of III MEF.

b. Information System Security Officer (ISSO). The Division G-6 Information Security Maintenance Officer (ISMO) serves as the Division ISSO and is responsible for the implementation and monitoring of Information Technology Equipment (ITE) security regulations and network security. These regulations are meant to ensure that the security needs of all TASO's and Users are met and to resolve any conflicts between systems. The ISSO is the highest element within the Division responsible for computer security.

c. Terminal Area Security Officer (TASO). Terminal Area Security Officers are responsible for the security and administration of all user, ITE hardware, ITE software, all host, Local Area Network (LAN), and Personal Computer resources accessible via the terminals in the terminal area which they exercise control. There are three levels of TASO's within the Division structure. The Division G-6 TASO reports to the Division G-6 ISSO and serves as the senior TASO within the Division. Each battalion/company is required to appoint a TASO and each staff section is required to appoint a TASO. The battalion, company, and staff section TASO's are subordinate to the Division TASO.

d. User. A user is a Marine that uses Information Technology Equipment for government use.

e. Control Zone. A control zone is a grouping of users within a command or section administered by a single TASO.

f. Computer Security. The technological safeguards and managerial procedures which can be applied to computer hardware, programs, data, facilities and workspaces to assure the availability, integrity and confidentiality of computer based resources.

g. TSS. TSS is an abbreviation for "TOP SECRET" security software

h. ACID. ACID is the acronym for "accessor ID". An ACID refers to any names data structure in the TOP SECRET SOFTWARE

id

Host
H

Appointment of TASO s

mp

p:

A.

mb

Separation of Duties
T TASO

User Identifiers (User IDs or ACIDS)

Structure

id

Accountability
hi tab.

p:

id

d:

name for an ACID. If the ACID is not assigned, the name field will have the word VACANT in it and the ACID will be suspended.

c. Group ACIDS. Group ACIDS, (ACIDS allowing more than one user access to it), are not permitted. Violators will be immediately suspended.

8 Password Control

a. The issuance of a user ACID to an individual requires that the user's ACID password be protected from disclosure and immediately changed should the password be compromised. The unauthorized disclosure of a password or use of another individual's ACID, are violations of the Computer Fraud and Abuse Act of 1986, and may punishable under Chapter 47 of Title 18 of the United States Code and under the UCMJ.

b. No one is permitted to list or look at passwords

c. Any TASO who needs to establish or reset a password, will set it to a nontrivial, unique password, and set it to expire

9. Security Indoctrination and Training. Some of the most effective features of a security program are training and indoctrination. Computer security awareness encompasses formal and informal training to ensure that all personnel involved in the use and management of computer resources understand and can implement their respective security responsibilities for safeguarding sensitive unclassified data derived from computer systems. Awareness training must be provided to new personnel, refreshed annually, and tailored to the types of responsibilities applicable to those personnel.

10. User Responsibility

a. Every user of a Personal Computer (PC) is responsible for protection of the data which the PC stores, processes, receives, or transmits. Physical access to a PC does not authorize the user to browse casually through another user's data. All PCs purchased by the Marine Corps are to be used only for authorized Marine Corps related activities. There is no presumption of privacy when using government owned automated data processing equipment. Reference (e) contains guidance on the authorized use of Marine Corps ADPE and E-mail policy. The Marine Corps retains the right to examine, at any time, data stored in a PC or on PC media.

b. The Marine Corps honors all licenses, copyrights, patents, restrictions and terms and conditions associated with commercial, proprietary computer software. Personnel are not authorized to copy (other than for backup), modify or transfer purchased computer programs. "Pirating" (making unauthorized copies of software) is a violation of copyright laws, and personnel are subject to indictment and conviction if found guilty. Unauthorized copies are illegal even if they are used only for the government job and never taken home for personal use.

11. Action

a. Assistant Chief of Staff, G-6

(1) Exercise primary staff cognizance over all computer security issues.

Appoint a Division ISSO in writing.

b. Division ISSO

(1) Implement and monitor ITE security regulations and network security.

(2) Determine what standard "security operating procedures" defined in the references are applicable to the Division and publish standard operating procedures.

(3) Conduct periodic surveys and reviews to determine compliance with security directives.

(4) Continuously review and evaluate the security impact of local network users.

Appoint a Division TASO in writing.

c. Division TASO

1 Be knowledgeable of the policies contained in the references

(2) Ensure local compliance with security instructions and operating procedures directed by the ISSO.

Manage and control the dissemination of USER ID's and
PASSWORDS

4) Assist the Division ISSO in ensuring overall system security.

(5) Report to the Division ISSO all potentially compromising practices to the overall security, and all instances of security violations.

(6) Assume responsibility for data obtained from the mainframe/3270 and downloaded to the Local Area Network (LAN) or personal computer (PC) within your control zone.

(7) Forward all security matters that cannot be resolved within your scope of authority to the Division ISSO.

(8) Know who your users and TASO's are. Be able to identify them visually.

(9) Conduct training for unit and section TASO's and coordinate with MCB for base sponsored TASO training. Maintain training records for 2 years.

(10) Issue ID's only to those individuals who have a "need to know" for specific applications.

(11) Prior to issuing a user ID, ensure that users are counseled as to their responsibilities associated with access privileges and the consequences of their abuse. Each user must read the Computer Fraud and Abuse Act of 1986 provided in enclosure (3).

(12) Attend the MCB TASO training course within two months of appointment.

d. Commanders and Principle Staff

Appoint a TASO in writing

(2) Ensure that a new TASO is appointed in writing prior to execution of Permanent Change of Station (PCS), Temporary Assigned Duty (TAD) or Fleet Assistance Program (FAP) orders by the current TASO.

(3) Ensure that TASO's have physical access to all spaces where users gain access to Automated Information Systems (AIS).

26 JAN 2000

(4) Ensure that TASO's have access via terminal to every to which every one of the users he/she administers has access.

(5) Ensure that new personnel receive "new join" indoctrination training and annual refresher training for Computer Security Awareness.

e. Battalion/Company/Staff Section TASO's

1 Be knowledgeable of the policies contained in the references

(2) Ensure local compliance with security instructions operating procedures directed by the ISSO.

(3) Manage and control the dissemination of USER ID's and PASSWORDS.

(4 Assist the Division ISSO in ensuring overall system security

(5) Report to the Division TASO all potentially compromising practices to the overall security, and all instances of security violations.

(6) Assume responsibility for data obtained from the mainframe/3270 and downloaded to the LAN or PC within your control zone.

(7) Forward all security matters that cannot be resolved within your scope of authority to the Division TASO.

(8 Know who your users are. Be able to identify them visually

(9) Attend TASO training within two months of appointment.

(10) Issue ID's only to those individuals who have a "need to know" for specific applications.

(11) Prior to issuing a user ID, ensure that users are counseled as to their responsibilities associated with access privileges and the consequences of their abuse. Each user must read the Computer Fraud and Abuse Act of 1986 provided in enclosure (3).

26 JAN 2000

(12) Conduct "new join" and annual refresher training for all unit personnel covering computer security awareness.

(13) Know the identity and how to contact the Division ISSO and Division TASO for assistance.

(14) Ensure that each terminal user's identity, need to know, level of clearance, and access authorization are established commensurate with the data accessible from that terminal.

(15) In coordination with your unit S-6, help prepare your unit/section for the Logistical Readiness Inspection (LRI) ITE inspection using the ITE inspection checklist provided in the CG Policy Letter 1-99.

f. Users

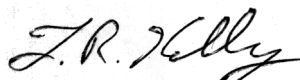
(1) Comply with all security operating practices directed by the Division ISSO.

(2) Assume responsibility for data obtained from mainframe/3270 and downloaded to the local area network (LAN) or PC.

(3) Know the identity and how to contact your TASO for assistance.

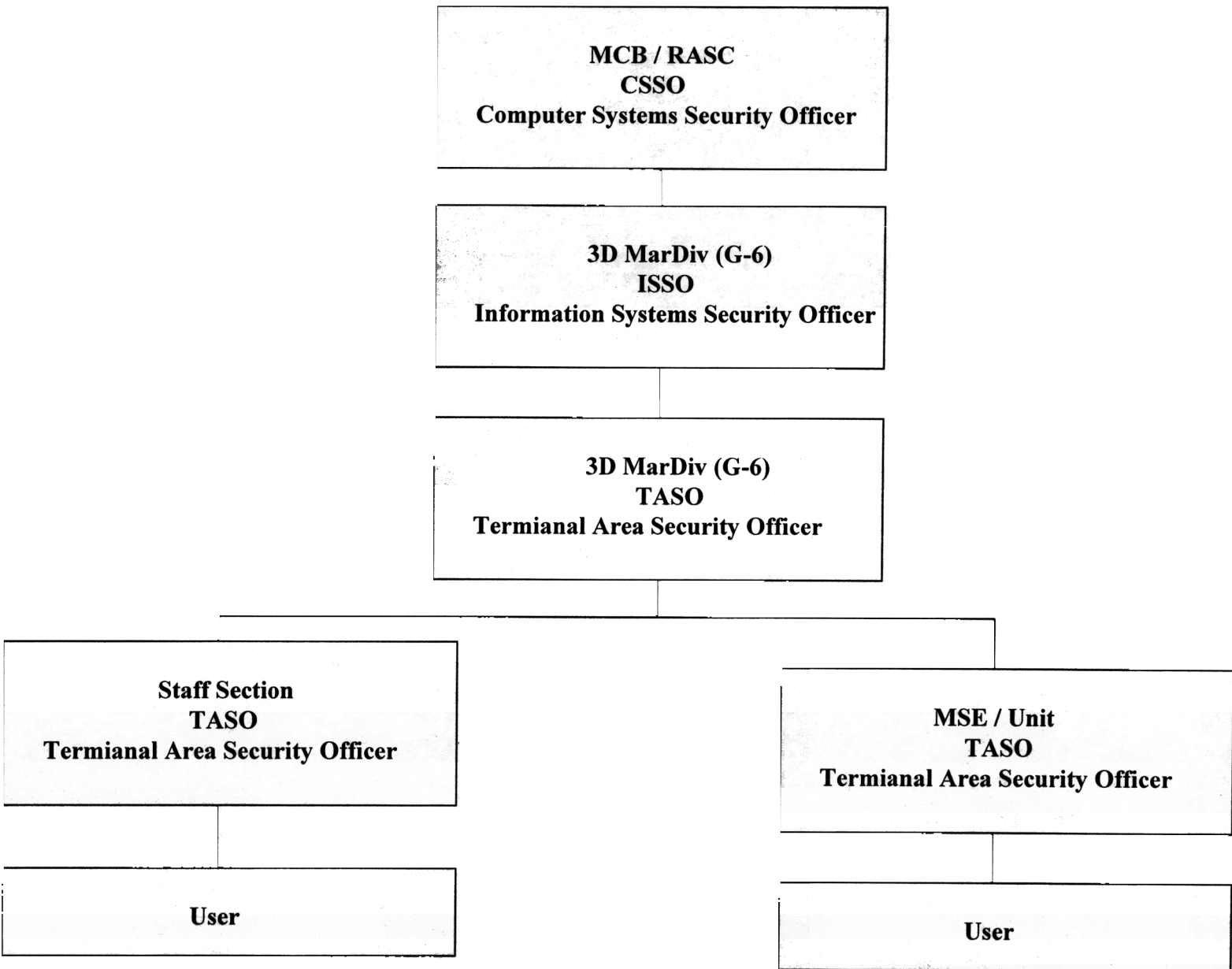
(4) Prior to receiving a USER ID, users must be counseled as to their responsibilities associated with access privilege and the consequences of their abuse.

(5) All users must read and sign the Computer Fraud and Abuse Act of 1986 provided in enclosure (3).



T. R. KELLY
Chief of Staff

DISTRIBUTION:



Sample TASO Appointment Letter

ORGANIZATIONAL HEADING

5510
CODE
DATE

From: Commanding Officer
To: Marine, D. D. 123 45 6789/XXXX/USMC
Subj: APPOINTMENT AS TERMINAL AREA SECURITY OFFICER (TASO)
Ref: (a) MCO P5510.14
(b) IRM 5239-06 Data Access Security
(c) Computer Fraud and Abuse Act of 1986
(d) IRM 5234-04 Naming Conventions

1. You are hereby appointed as the TASO for UNIT. Your TASO ACID is DIXXXX. You are to thoroughly familiarize yourself with reference (a) through (d). This appointment will remain in effect until you are formally relieved.

2. The CSSO's of the following ADP activities have been notified of this change of appointment: OKR, KCT, MQG.

Signature of CO

CODE
DATE

From: Marine, D. D. 123 45 6789/XXXX/USMC
To: Commanding Officer

Subj: TASO APPOINTMENT LETTER

1. I have read and understand references (a) through (d) and have assumed all duties in conjunction with my appointment to TASO.

2. My RTD is YYMMDD and my DSN phone number is ###-####

D. D. MARINE

ENCLOSURE (2)

COMPUTER FRAUD AND ABUSE ACT OF 1986

1. The below is a paraphrased version of the Computer Fraud and Abuse Act of 1986 (Public Law 99-474). The sections of the act not covered below concern classified information and information subject to the Atomic Energy Act of 1954, the Right to Financial Privacy Act of 1978, and the Fair Credit Reporting Act.

Public law 99-474, chapter XXI, Section 1030, states that "whoever knowingly ..., or intentionally accesses a computer without authorization or exceeds authorized access, and by means of such conduct, ...obtains..., alters, damages, destroys, or discloses information ..., or prevents authorized use of (data or a computer owned by or operated for) the government of the United States ... shall be punished (by) ... a fine under this title or imprisonment for not more than 10 years, or both".

2. All end users are required to read this Act as a part of their security brief before they are issued a User ID.

3. I have read and understand public law 99-474.

Signature/Date